

Strong Customer Authentication for Apple Pay on iPhone with A12 Bionic running iOS 14.5.1

Guidance

Version 1.4

November 23, 2021

Apple
One Apple Park Way
Cupertino, CA 95014

Table of Contents

1. Introduction	3
2. Preparation Guidance	4
3. Identification	4
4. Operational Guidance	4
4.1. Configure Passcode	4
4.2. Configure Face ID	5
4.3. Update iOS	5
4.4. Apple Pay	5
4.5. Apple Cash	6
4.6. Operational failures	6
Annex A - Issuer Security Objectives	7
Annex B - Apple Server Security Objectives	9

1. Introduction

This document contains references to other documents providing guidance for security related topics specified in the Security Target.

Reference	Description
[APC]	Send and receive money with Apple Cash https://support.apple.com/explore/apple-pay-cash
[AP]	Apple Pay Support https://support.apple.com/apple-pay
[ENROLLAP]	Set up Apple Pay https://support.apple.com/en-us/HT204506
[ENROLLAPC]	Set up Apple Cash and person to person payments https://support.apple.com/en-us/HT207886
[INITCFG]	Set up your iPhone, iPad, or iPod touch https://support.apple.com/en-us/HT202033
[APS]	Apple Platform Security https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
[IOSUPDATE]	Update the iOS on your iPhone, iPad, or iPod touch https://support.apple.com/en-us/HT204204
[PASSCODE]	Use a passcode with your iPhone, iPad, or iPod touch https://support.apple.com/en-us/HT204060
[PASSCODE_POLICY]	Passcode policies for iPhone and iPad deployment https://support.apple.com/en-gb/guide/deployment-reference-ios/ior975e176c6/web
[FACEID]	Use Face ID on your iPhone or iPad Pro https://support.apple.com/en-us/HT208109
[IOSSLA]	A. Apple iOS Software License Agreement B. Apple Pay Supplemental Terms and Conditions https://www.apple.com/legal/sla/docs/iOS14_iPadOS14.pdf
[IPHONEID]	Identify your iPhone model https://support.apple.com/en-us/HT201296
[IOSID]	Find the software version on your iPhone, iPad, or iPod https://support.apple.com/en-us/HT201685
[FACEID_NotWork]	Face ID not working on iPhone https://support.apple.com/en-us/HT208114
[DISABLE]	iPhone disabled mode https://support.apple.com/en-us/HT204306

2. Preparation Guidance

After unpacking and powering up the device for the first time, or after a complete erase, the iOS device presents a set of questions to the user as outlined in [INITCFG].

As part of the initial configuration, the user is asked to configure a passcode and enroll into Face ID biometric authentication.

After completion of the initial installation steps, the user is able to enroll into Apple Pay and Apple Cash. The enrollment process is illustrated at [ENROLLAP]. To enable Apple Cash, the guidance given at [ENROLLAPC] should be consulted.

3. Identification

Two guides [IPHONEID] and [IOSID] are provided for identifying the device model and the installed software:

The following identifiers correspond to the TOE:

- Model: iPhone XR, iPhone XS, or iPhone XS Max.
- iOS version: "14.5.1"

4. Operational Guidance

In addition to the initial configuration steps, various use cases and options are available for the security functions at runtime. All security related mechanisms are documented as follows.

In general, all security features of iOS devices including authentication, system updates, Apple Pay, and Apple Cash are documented in [APS]. In addition, specific user guidance is given in the documents referenced in subsequent sections of this document.

Apple provides a high-level document covering the iOS Software License and Agreement [IOSSLA], including supplemental terms and conditions for the use of Apple Pay services (Apple Pay and Apple Cash).

4.1. Configure Passcode

Managing the passcode is provided with the configuration user interface specified in [PASSCODE]. The guidance provides details about adding, changing, and removing a passcode.

The user can choose from an extensive set of passcode policies to meet their security needs [PASSCODE_POLICY]. These passcode policies can include requirements for:

- A passcode on an iPhone
- An alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Time before auto-lock
- Passcode history (unable to use previous passwords)
- Grace period for device lock
- Maximum number of failed attempts before an iPhone or iPad is erased

When using Apple Pay the user should select a complex passcode and protect it well. They should avoid writing it down and using obvious values such as date of birth that a third party might guess.

4.2. Configure Face ID

iOS allows the configuration of Face ID by allowing users to enroll their face (up to two enrollments of a user's face if the user enables the use of an alternate appearance), and removal of all enrolled faces. All configuration steps pertaining to these actions are given in [FACEID].

This guidance documentation also provides information about how Face ID is used to unlock the device and during Apple Pay and Apple Cash transactions.

4.3. Update iOS

The iOS operating system can be updated following the steps provided in [IOSUPDATE].

iOS updates include all software and firmware relevant to Apple Pay and Apple Cash.

4.4. Apple Pay

With Apple Pay, users can enroll credit cards and debit cards to perform transactions using an iOS mobile device. All transactions and usage scenarios that can be performed with Apple Pay are detailed in [AP].

Security Note: User SHALL NEVER perform Apple Pay card provisioning on a device that is plugged into another piece of equipment.

4.5. Apple Cash

Apple Cash allows a number of different operations, including payments and transfer of money from a debit card to Apple Cash. All aspects related to Apple Cash are documented in [APC].

4.6. Operational failures

Two guides [FACEID_NotWork] and [DISABLE] are provided for handling the device in cases where:

- Face ID does not work
- User forgets the passcode
- Device is disabled

Annex A - Issuer Security Objectives

For Apple Pay services (Apple Pay and Apple Cash), the Issuer or its service provider is the third party in charge of:

- Management of user data for Apple Pay services
- Management of user data for Apple Cash services
- Processing Apple Pay transactions
- Processing Apple Cash transfers

The Issuers authorized to provision cards (for their card holders, or to the card holders of their affiliates) enforce the following Security Objectives:

Environment Security Objectives	Description
Card Holder and Apple Pay/Apple Cash Perso	The Issuer is responsible for verifying that the User is authorized to perform a transaction on the account of the card used as a reference, before allowing the Apple Pay/Apple Cash card personalization. The Issuer also ensures the robustness of the personalization data, to prevent attacks like forgery, counterfeit or corruption.
Card Data	The Issuer is responsible for using the appropriate security measures to protect the confidentiality and the integrity of the Apple Pay/Apple Cash card's sensitive data and guarantee the authenticity of card data during enrolment.
Card Delete	The Issuers of all Apple Pay and Apple Cash cards installed on a device are informed when the User removes a card from that device, removes that device from the iCloud account or performs a device Erase All Content and Settings. The Issuers ensure these cards are removed from the User's account (i.e. the unlinking process of the DPAN from the FPAN, which is done by the Issuer or the corresponding TSP).
Apple Pay Transaction Verification	The Issuers ensure that the cryptogram released by the Apple Pay device, for an Apple Pay transaction with an Apple Pay/Apple Cash card they provisioned, is verified before the payment proceeds. The cryptogram validation result allows the Issuer to approve or reject the transaction. The payment is invalidated if this verification fails.
Statement	The Apple Pay card Issuers ensure that the statement associated to an Apple Pay card (list of transactions) is fully accurate and includes, but is not restricted to, the amount and recipient of each transaction. The Apple Cash Issuer ensures that the ledger associated to an Apple Cash account (list of transfers including completed/canceled/pending) is fully accurate.
Dynamic Linking	For eCommerce transactions, the Issuer verifies the cryptographic based dynamic linking of the transaction data (including amount and payee). The payment is invalidated if this verification fails.

CDCVM	Payment networks or issuers are responsible for ensuring that Express transactions can only be accepted for transit-specific use by requiring that non-transit Apple Pay payment transactions have a successful CDCVM.
-------	--

Annex B - Apple Server Security Objectives

Apple servers are in charge of:

- Management of a User's iCloud account
- Management of User enrollment in Apple Pay
- Management of User enrollment in Apple Cash
- Management of iOS releases
- Device's interface for processing Apple Pay transactions (contact S.Issuer)
- Device's interface for processing Apple Cash transfers (contact S.Issuer)

Apple servers enforce a range of security objectives:

Environment Security Objectives	Description
Anti-Replay	The Apple Pay server verifies that each payment (e-Commerce Apple Pay transaction or Apple Cash transfer) is not replayed. The payment is invalidated if this verification fails.
Apple Cash Transaction Verification	The Apple Pay server ensures that no Apple Cash transfer can be executed if the submitted quote (received by the server before the User approves) does not match the transaction data (received by the server once the device completes transfer processing). The modifications that the server is able to detect cover but are not limited to, modification on the amount and the recipient.
Dynamic Linking	For eCommerce transactions, the Apple Pay server preserves the cryptographic based dynamic linking of the transaction data (including amount and payee).
Genuine_Wallet	The Wallet application is provided and signed by Apple.

Change History

Date	Version	Author	Comments
2021-03-09	1.0	Apple	Version after comments of evaluation lab
2021-03-29	1.1	Apple	Updating iOS version
2021-08-12	1.2	Apple	Adding security recommendations
2021-10-20	1.3	Apple	Updates according to internal reviews
2021-11-23	1.4	Apple	Front page modification